

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-86441

(P2004-86441A)

(43) 公開日 平成16年3月18日 (2004. 3. 18)

(51) Int. Cl. ⁷

G06F 15/00

G06F 17/60

H04B 7/28

H04Q 7/20

F I

G06F 15/00 330Z

G06F 15/00 330D

G06F 17/60 326

G06F 17/60 506

G06F 17/60 512

テーマコード (参考)

5B085

5K067

審査請求 有 請求項の数 10 O L (全 15 頁) 最終頁に続く

(21) 出願番号 特願2002-245061 (P2002-245061)

(22) 出願日 平成14年8月26日 (2002. 8. 26)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ

東京都江東区豊洲三丁目3番3号

(74) 代理人 100095371

弁理士 上村 輝之

(72) 発明者 藤原 仁

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

(72) 発明者 吉野 順

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

Fターム (参考) 5B085 AA08 BG02 BG03 BG07

5K067 AA21 BB04 BB21 DD43 GG22

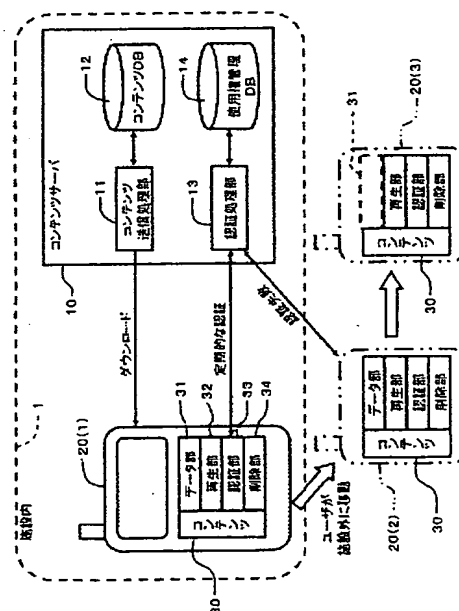
HH22 JJ43 JJ52

(54) 【発明の名称】 コンテンツ管理システム

(57) 【要約】

【課題】 所定の圏内に位置する情報端末でのみコンテンツデータの閲覧や試聴を許可できるようにすること。

【解決手段】 店舗や図書館あるいは学校等の施設1内に位置するユーザは、自分の情報端末20内にサーバ10からダウンロードしたコンテンツデータ30を格納する。コンテンツデータ30中の認証部33は、サーバ10との間で定期的な認証を行う。認証が失敗した場合は、端末20が施設1外に出たものと判定され、端末20に格納されたコンテンツデータの全部又は一部が削除され、その利用が禁止される。



【特許請求の範囲】

【請求項1】

コンテンツデータを管理するコンテンツ管理装置からユーザの情報端末に供給されるコンテンツデータを管理するコンテンツ管理システムにおいて、前記情報端末が前記コンテンツ管理装置と通信可能な圏内に位置するか否かを判定する判定手段と、前記判定手段により前記情報端末が前記圏内に位置すると判定された場合は、前記情報端末に供給された前記コンテンツデータの利用を許可し、前記判定手段により前記情報端末が前記圏外に位置すると判定された場合は、前記情報端末に供給された前記コンテンツデータの利用を禁止させる制御手段と、を備えたことを特徴とするコンテンツ管理システム。

【請求項2】

前記判定手段は、前記情報端末と前記コンテンツ管理装置との間で定期的な通信を行わせ、予定された通信が正常に完了したか否かを検出することにより、前記判定を行うものである請求項1に記載のコンテンツ管理システム。

【請求項3】

前記制御手段は、前記情報端末が前記圏外に位置すると判定された場合は、前記情報端末に供給された前記コンテンツデータの全部又は一部を削除することにより、前記コンテンツデータの利用を禁止させるものである請求項2に記載のコンテンツ管理システム。

【請求項4】

前記制御手段は、前記情報端末が前記圏外に位置すると判定された場合、前記情報端末が前記コンテンツデータを再生中であるか否かを検査し、前記コンテンツデータの再生中である場合は、当該再生が終了した後で、前記コンテンツデータの利用を禁止させるものである請求項3に記載のコンテンツ管理システム。

【請求項5】

前記判定手段及び前記制御手段は、前記情報端末内で実行されるものである請求項4に記載のコンテンツ管理システム。

【請求項6】

前記判定手段及び前記制御手段は、前記コンテンツデータ内に予め設けられており、前記コンテンツデータが前記情報端末内に格納されることにより、それぞれ実行されるものである請求項5に記載のコンテンツ管理システム。

【請求項7】

前記情報端末と前記コンテンツ管理装置とは、近距離無線LAN (Local Area Network) を介して双方向通信が可能である請求項6に記載のコンテンツ管理システム。

【請求項8】

前記コンテンツデータは、前記近距離無線LANを介し

て前記情報端末に送信され、前記情報端末内に格納されるものである請求項7に記載のコンテンツ管理システム。

【請求項9】

前記コンテンツデータは、記録媒体を介して前記情報端末に供給されるものである請求項7に記載のコンテンツ管理システム。

【請求項10】

コンテンツ管理装置からユーザの情報端末に供給されるコンテンツデータを管理するためのプログラムであって、前記コンテンツデータを復号化して再生させる機能と、前記情報端末が前記通信ネットワークを介して前記コンテンツ管理装置と通信可能な圏内に位置するか否かを判定する判定機能と、前記情報端末が前記圏内に位置すると判定された場合は、前記コンテンツデータの利用を許可し、前記情報端末が前記圏外に位置すると判定された場合は、前記コンテンツデータの利用を禁止させる機能と、をコンピュータ上で実現させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えば、図書館、書店、音楽CD店、レンタルビデオ店等の各種施設内で映像データ等のコンテンツデータをユーザの情報端末に供給して試聴等させることができるコンテンツ管理システムに関する。

【0002】

【従来の技術】

コンピュータ技術及びネットワーク技術の進展に伴い、例えば、書籍、映画、音楽等の各種コンテンツが、文字データ、静止画像データ、動画像データ、音楽データ等としてデジタル化されている。これらデジタル化されたコンテンツは、例えば、通信ネットワークを介して端末に配信されたり、DVD-ROM等の記録媒体に固定されて配布等されている。

【0003】

デジタル化されたコンテンツは、例えばインターネット等の通信ネットワークを介して容易にユーザの端末に配信することができる。従って、ネットワーク上の仮想店舗でデジタルコンテンツを販売することが可能であり、仮想店舗によるコンテンツデータの販売は急速に普及している。

【0004】

ここで、サーバからコンテンツデータを配信する方式としては、ダウンロード方式とストリーミング方式とが知られている。ダウンロード方式は、コンテンツデータの全体を端末の記憶装置に格納させてから再生させるものであり、蓄積型の配信方法である。これに対し、ストリーミング方式は、非蓄積型の配信方法であり、端末は、

小分けされたコンテンツデータのブロックを受信しながら再生を開始し、再生済みのデータを破棄していくものである。

【0005】

ダウンロード方式では、コンテンツデータの全体を端末の記憶装置に格納させるため、格納完了までの待ち時間が生じる。しかし、いったん保存したコンテンツは、特に制限を受けない限り、何度でも再生して楽しむことができる。一方、ストリーミング方式の場合は、再生開始までの待ち時間を最小に抑えることができるが、再生済みのデータを次々に破棄していくため、何度も繰り返して再生する場合は、その度にサーバにアクセスしてコンテンツデータを受信しなければならない。

【0006】

【発明が解決しようとする課題】

上述の通り、デジタル化されたコンテンツは、コンピュータ通信と馴染みやすく、仮想店舗を通じた販売等が行われやすい。しかし、デジタル化されたコンテンツの全てがネットワークを介して無店舗で貸与されたり販売等されたりするわけではなく、現実の店舗等の施設内で、デジタルコンテンツが販売されたり貸与される場合も考えられる。例えば、図書館内のLANを介して端末に書籍や映像のコンテンツデータを配信し、館内のユーザに閲覧させたり、あるいは、本屋や音楽CD店等で、商品である書籍や音楽のコンテンツデータを端末に配信して試聴させたりするような場合である。なお、コンテンツデータは、施設内のLANを介して供給される場合に限らず、CD-ROMやDVD-ROM等の記録媒体を介してユーザに供給されることもある。

【0007】

このように実際の施設内でデジタルコンテンツを配信するには、端末に配信したコンテンツデータの管理が特に重要となる。デジタルデータは、コピーが容易で、コピーとオリジナルとの品質的な差もないためである。

【0008】

そこで、1つの方法として、施設内にデジタルコンテンツ再生用の専用端末を設置し、専用端末を介してユーザに試聴や閲覧等させることが考えられる。専用端末であるため、端末内のコンテンツデータをユーザが無断で持ち出すことは通常不可能であり、データ管理の点からは優れている。しかしその反面、専用端末は一般に汎用の端末より高価なため、初期費用や維持費用等がかさむ。また、専用端末の設置台数が少ない場合は、多数のユーザに同時に試聴等させることができず、ユーザの待ち時間が増大して、顧客満足度が低下する。逆に、専用端末を予め十分多く設置すると、費用がかさむ上に、ユーザ数の少ない時間帯等では専用端末の稼働率が低下する。つまり、専用端末方式は、需要の変化に柔軟に対応することができず、費用面で問題を抱える。

【0009】

他の方法として、パーソナルコンピュータやPDA(Personal Digital Assistant)等の汎用の端末を採用し、汎用端末に施設内のサーバからLANを介してコンテンツデータを配信することも考えられる。汎用端末方式では、ユーザが持ち込んだ汎用端末を利用することもできるため、専用端末方式よりも費用面で大幅に有利である。しかし反面、ユーザが持参した汎用端末にコンテンツデータを保存して試聴や閲覧等を行わせることも可能なため、コンテンツデータの管理が難しく、施設外にコンテンツデータを持ち出されてしまう可能性がある。

【0010】

そこで、コンテンツデータの再生回数や再生可能時期を予めコンテンツデータ内に設定しておくことにより、ユーザの汎用端末に保存されたコンテンツデータを管理する方法も考えられる。再生回数や再生可能時期の制限により、コンテンツデータのある程度管理することができる。

【0011】

しかし、再生回数や再生可能時期という条件自体は、そのコンテンツデータを供給した施設(図書館や店舗等)との関連性が無い。従って、例えば、施設を訪れたユーザのみにコンテンツデータの試聴等を許可したい場合や、施設内での販売に結びつけるために試聴等を許可したい場合等のような要求に応えることができないという問題がある。つまり、施設の運営者がその施設内でのみコンテンツデータの供給を行いたい場合には、従来の方法はそのまま採用できない。

【0012】

本発明は、上記の課題に鑑みてなされたものであり、その目的は、所定の圏内でのみコンテンツデータを利用できるようにしたコンテンツ管理システムを提供することにある。本発明の他の目的は、後述する実施の形態の記載から明らかになるであろう。

【0013】

【課題を解決するための手段】

上記課題を解決するため、本発明に係るコンテンツ管理システムは、コンテンツ管理装置からユーザの情報端末に供給されるコンテンツデータを管理するものであって、判定手段と制御手段とを備えている。

【0014】

判定手段は、情報端末がコンテンツ管理装置と通信可能な圏内に位置するか否かを判定する。制御手段は、判定手段により情報端末が圏内に位置すると判定された場合は、情報端末に供給されたコンテンツデータの利用を許可し、判定手段により情報端末が圏外に位置すると判定された場合は、情報端末に供給されたコンテンツデータの利用を禁止させる。

【0015】

ここで、「コンテンツ管理装置」は、例えば、図書館、

学校、コンビニエンスストアや量販店等の各種店舗、駅、空港、銀行、病院、ホテル、行政庁舎等の施設内に又は施設に関連づけられて設けられる。具体的には、コンテンツ管理装置を各施設内にそれぞれ設置してもよいし、あるいは、1台又は複数台のサーバで1カ所又は複数箇所の施設にコンテンツデータを送信する等のように、施設外に設置したコンテンツ管理装置によりコンテンツデータを管理してもよい。情報端末とコンテンツ管理装置は、通信ネットワークを介して双方向通信を行うことができる。通信ネットワークとしては、例えば、LANや移動体通信を挙げることができる。LANは、有線接続、無線接続どちらでもよい。「情報端末とサーバとが通信可能な圏内」は、例えば、壁や家具等の配置、無線LANアクセスポイントやハブの設置場所等によっても相違するが、施設の建物又は敷地とほぼ一致する場合のほか、建物や敷地内の一部でのみ通信可能な場合、通信可能な圏内が建物や敷地の外部に及ぶ場合もある。「コンテンツデータ」としては、例えば、書籍、音楽、映画、ドラマ、ニュース、テレビジョン番組、ラジオ番組等を挙げることができる。

【0016】

制御手段は、情報端末が所定の圏内にある場合にコンテンツデータの利用を許可し、情報端末が圏外に出た場合はコンテンツデータの利用を禁止させる。これにより、施設と関連づけて、ユーザにコンテンツデータを利用させることができる。ここで、コンテンツデータは、情報端末の記憶装置（メモリやハードディスク装置等）にいったん保存されるが、コンテンツデータの配信に際しては、いわゆるストリーミング方式を採用し、受信した部分から直ちに再生するようにしてもよい。あるいは、コンテンツデータは記録媒体に記録された状態で、情報端末に供給される場合もある。

【0017】

本発明の一態様では、判定手段は、情報端末とコンテンツ管理装置との間で定期的な通信を行わせ、予定された通信が正常に完了したか否かを検出することにより、判定を行うようになっている。

【0018】

コンテンツ管理装置と情報端末との間で定期的な通信を行わせることにより、2つのコンピュータ間での接続が維持されているか否かに基づいて、情報端末が所定の圏内にあるか否かを判定することができる。

【0019】

本発明の一態様では、制御手段は、情報端末が圏外に位置すると判定された場合は、情報端末に供給されたコンテンツデータの全部又は一部を削除することにより、コンテンツデータの利用を禁止させる。

【0020】

コンテンツデータの全体を削除してしまえば、その後コンテンツデータを利用することはできなくなる。あるいは

は、コンテンツデータが暗号化されている場合に復号化キーのデータのみを削除する等のように、コンテンツデータの一部を削除するだけでも、コンテンツデータの利用を禁止させることができる。さらに、コンテンツデータの全体からランダムに又は所定の規則の下にデータを間引きすることにより、コンテンツデータの利用を禁止してもよい。コンテンツデータの一部を削除する場合は、削除部分のみを情報端末が再取得することにより、コンテンツデータを再利用できるため、再利用時のデータ受信時間を短縮することができる。

【0021】

本発明の一態様では、制御手段は、情報端末が圏外に位置すると判定された場合、情報端末がコンテンツデータを再生中であるか否かを検査し、コンテンツデータの再生中である場合は、当該再生が終了した後で、コンテンツデータの利用を禁止させる。

【0022】

例えば、情報端末でコンテンツデータを再生中のユーザが、所用で一時的に圏外に出たような場合に、直ちにコンテンツデータの利用を禁止せず、現在の再生が終了するまで猶予を与える。

【0023】

判定手段及び制御手段は、情報端末内で実行することができる。

【0024】

さらに、判定手段及び制御手段は、コンテンツデータ内に予め設けられており、コンテンツデータが情報端末内に格納されることにより、それぞれ実行されるように構成することができる。

【0025】

即ち、判定手段及び制御手段をコンピュータプログラムとして構成し、このプログラムをコンテンツデータ内に含めて情報端末に供給し、情報端末内で実行させる。

【0026】

なお、コンテンツデータは、近距離無線LAN又は記録媒体を介して情報端末に供給することができる。あるいは、コンテンツデータの一部は無線LANを介して情報端末に供給し、残りのコンテンツデータは記録媒体を介して情報端末に供給する場合もあり得る。

【0027】

本発明は、コンピュータプログラムの発明として把握することもでき、コンピュータプログラムは、例えば、CD-ROM、DVD-ROM、メモリ、ハードディスク、磁気テープ等の記録媒体に記録して配布できるほか、通信ネットワークを介しても配信することができる。

【0028】

【発明の実施の形態】

以下、図1～図8に基づき本発明の実施の形態について詳述する。

【0029】

1. 第1の実施の形態

【0030】

まず、図1～図6は本発明の第1の実施の形態に係る。図1は、コンテンツ管理システムの全体概要を示す機能ブロック図であって、例えば、図書館や店舗等の施設1には、コンテンツサーバ10（以下、「サーバ10」と略記）が設けられており、施設内のユーザは、自分の情報端末20にサーバ10から送信されたコンテンツデータを保存して再生することにより、コンテンツの試用（一時的限定的な視聴等）が行えるようになっている。以下、施設1の一例として、書籍や音楽ディスクの販売を行う店舗を例に説明する。

【0031】

サーバ10は、コンテンツ送信処理部11、コンテンツデータベース（図中では「DB」と略記）12、認証処理部13及び使用権管理データベース14を備えている。なお、サーバ10は、各施設1のそれぞれに個別に設置することもできるし、あるいは、本店や本部等の施設1の外部に設置したサーバ10によって、複数の支店や加盟店等でコンテンツデータの配信サービスをそれぞれ行うようにすることもできる。また、サーバ10は、1台のコンピュータから構成される必要はなく、複数のコンピュータを連係動作させて構成してもよい。

【0032】

コンテンツ送信処理部11は、情報端末20からの要求に応じたコンテンツデータ又は予め設定されたコンテンツデータを、コンテンツデータベース12から読出し、ハブや無線LANアクセスポイント等を介して、情報端末20に送信するものである。例えば、キャンペーン中のコンテンツの場合は、情報端末20からの要求の有無を問わずにコンテンツデータを送信するように構成することができ、この場合、ユーザの同意を得るのが望ましいが、これに限らず、場合によっては、ユーザの同意を確認する前に、又はユーザの同意を得ることなく、コンテンツデータを送信する構成としてもよい。

【0033】

認証処理部13は、後述する情報端末20側からの要求に応じて、認証処理を行うものである。本実施の形態では、後述のように、ユーザ認証（正当な権限を有するユーザであるか否かの認証）、端末認証（正当な権限を有する端末であるか否かの認証）及び端末位置認証（所定のエリアに端末が位置するか否かの認証であり、エリア認証と呼ぶこともできる）の3種類の認証を行っている点に留意すべきである。コンテンツデータベース12及び使用権管理データベース14については、図3と共に後述する。

【0034】

ユーザが所持する情報端末20は、例えば、パーソナルコンピュータ、PDA、携帯電話、音楽プレイヤー、デ

ジタルカメラ、ディジタルビデオカメラ等として実現されるものである。即ち、情報端末20は、コンテンツデータを記憶する記憶機能、コンテンツデータの再生処理等のデータ処理を行うデータ処理機能、サーバ10との間で双方向のデータ通信を行う通信機能、再生されたコンテンツデータを視覚や聴覚等でユーザに提供するユーザインターフェース機能を備えていればよい。また、情報端末20は、ユーザの所有物である必要はなく、施設1側から貸与されるものでもよい。

【0035】

情報端末20は、サーバ10から受信したコンテンツデータ30を保存して再生する。コンテンツデータ30は、文字データや音楽データあるいは画像データ等からなるデータ部31と、データ部31を再生するための再生部32と、サーバ10との間で認証を行うための認証部33と、コンテンツデータ30の全体又は復号化キーデータのみを削除するための削除部34とを備えている。再生部32、認証部33及び削除部34は、情報端末20内にダウンロードされ、情報端末の演算処理装置により実行されるプログラムである。

【0036】

図1中に「情報端末20（1）」として示すように、情報端末20を所持するユーザが施設1内に居る間は、情報端末20の認証部33とサーバ10の認証処理部13との間で定期的な認証が行われる。この認証が成功している間は、情報端末20がサーバ10との通信エリア内に存在するものと判定され、再生部32はデータ部31を再生する。「情報端末20（2）」として示すように、ユーザが施設1の外部に出て、サーバ10との通信エリア外に移動すると、移動後に行われる最初の認証が失敗する。

【0037】

これにより、情報端末20が通信エリア外に出たことを認証部33が検出し、「情報端末20（3）」として示すように、削除部34がコンテンツデータ30の全体を、又はデータ部31の再生に必要な復号化キーデータを削除する。なお、説明の便宜上、図1中では、データ部31のみを削除するかのように示しているが、本発明はこれに限定されない。通信エリア外におけるコンテンツデータの再生を禁止することができるよう、コンテンツデータ30の全部又は一部を削除すればよい。さらに、一部を削除する場合としては、復号化キーデータの削除、データ本体であるデータ部31の全部削除、データ部31の部分的な削除等を行うことができる。

【0038】

図2は、コンテンツデータ30及びライセンス40の関係を示す説明図であり、ディジタル化されたコンテンツデータ30は、一意に割り当てられた識別情報としてのコンテンツID（Identity）を有する。また、データ部31は所定の暗号アルゴリズムに基づいて暗号

化されており、その復号化のためには、ライセンス４０に含まれる復号化キーデータが必要とされる。

【００３９】

ライセンス４０は、コンテンツデータ３０を再生するために必要なデータである。ライセンス４０には、コンテンツデータ３０との対応関係を示すコンテンツＩＤと、データ部３１を復号化するためのキーデータと、コンテンツを再生するための条件とを含めることができる。

【００４０】

コンテンツ再生条件としては、例えば、再生可能回数、再生可能期間、視聴可能なページ数等を挙げることができる。これらのコンテンツ再生条件は、例えば、コンテンツのカテゴリー（音楽か書籍か等）、コンテンツのジャンル（音楽カテゴリー内の場合、軽音楽かクラシックか等）、コンテンツのデータサイズ、コンテンツ制作者やコンテンツ販売者の意向（例えば、キャンペーン期間中は視聴回数を増加させる等）に応じて、設定することができる。また、同一のコンテンツデータであっても、試用するユーザ毎にコンテンツ再生条件を設定することも可能である。例えば、その店舗での購入金額が多いユーザや、コンテンツがターゲットとする顧客層に属するユーザには、一般ユーザよりも長時間の視聴を許可することが可能である。

【００４１】

図３は、コンテンツデータベース１２及び使用権管理データベース１４の記憶内容の一例を示す説明図である。

【００４２】

図３（ａ）に示すコンテンツテーブル４１は、コンテンツデータベース１２に設けられるもので、例えば、コンテンツＩＤ、コンテンツの格納位置を示すパス（格納先アドレス）、コンテンツの説明、著作権管理情報、コンテンツの属するカテゴリー等を対応付けて管理している。

【００４３】

次に、図３（ｂ）～（ｇ）は、使用権管理データベース１４に記憶されるものであり、図３（ｂ）に示すコンテンツ使用権管理テーブル４２は、例えば、コンテンツＩＤ、復号キーデータ、試用可否フラグ、コンテンツ価格等を対応付けて管理している。試用可否フラグは、そのコンテンツの試用が許可されているか否かを示す情報である。

【００４４】

図３（ｃ）に示すユーザ管理テーブル４３は、例えば、各ユーザ毎に一意に割り振られたユーザＩＤとユーザ情報とを対応付けて管理している。ユーザ情報としては、例えば、ユーザの氏名、住所、電話番号、電子メールアドレス、職業、家族構成、趣味、過去の購入履歴等を挙げることができる。

【００４５】

図３（ｄ）に示す端末管理テーブル４４は、例えば、各情報端末２０毎に一意に割り当てられた端末ＩＤと端末

情報とを対応付けて管理している。端末情報としては、例えば、情報端末の種類（携帯電話かパーソナルコンピュータか）、製造メーカー名、機種名、データ処理能力（ＣＰＵ、メモリ量、搭載ＯＳの種類等）、データ通信能力（通信速度等）、ユーザインターフェースの能力（カラーディスプレイ搭載かモノクロディスプレイか等）を挙げることができる。

【００４６】

図３（ｅ）に示すコンテンツ使用条件管理テーブル４５は、例えば、コンテンツＩＤとコンテンツ再生条件とを対応付けて管理している。コンテンツ再生条件の具体例は、上述した通りである。

【００４７】

図３（ｆ）に示すコンテンツ購入管理テーブル４６は、例えば、ユーザＩＤとコンテンツＩＤと再生フラグとを対応付けて管理している。再生フラグは、コンテンツＩＤで特定されるコンテンツデータが現在再生中であるか否かを示す情報である。

【００４８】

図３（ｇ）に示す端末位置管理テーブル４７は、例えば、エリア情報とエリアの詳細情報とを対応付けて管理している。エリア情報とは、サーバ１０との通信可能エリアを特定する位置情報であり、例えば、通信可能エリアの住所、緯度経度等である。エリア情報により、情報端末２０がサーバ１０と通信可能な地域的範囲を知ることができる。また、エリアの詳細情報とは、サーバ１０と情報端末２０とが通信可能なエリアの詳細を記すもので、例えば、施設名称、施設管理者名、施設の構造（何階建てか等）、通信エリア内の通信不能場所（壁や家具、アクセスポイントの配置等により通信不能場所がある場合）等を挙げることができる。

【００４９】

次に、図４～図６に基づき、本実施の形態による各部の動作を説明する。以下、ステップを「Ｓ」と略記する。また、図に示すフローチャートは、処理動作の概要を示すものであって、実際のプログラムとは相違する場合がある。

【００５０】

図４は、情報端末２０に保存されたコンテンツデータ３０の再生部３２による再生処理のフローチャートである。

【００５１】

まず、使用権管理データベース１４を検索することにより、再生しようとするコンテンツデータが既に購入済みであるか否かを判定する（Ｓ１）。コンテンツデータがまだ購入されていない場合は（Ｓ１：ＮＯ）、再生が許可されている端末であるか否かを判定する（Ｓ２）。例えば、予め施設１内に設置された端末や施設１側がユーザに貸与した端末かユーザが持ち込んだ私物であるかを検査する。

【0052】

ユーザが施設1内に持ち込んだ私物の端末の場合は（S2：NO）、コンテンツの再生が許可されたエリア内に情報端末20が位置するか否かを判定する（S3）。図5に示す定期的に行われる認証処理が成功している間は、許可されたエリア内に位置するものとして判定される。

【0053】

このように、本実施の形態では、購入したユーザであるか否かのユーザ認証（S1）、再生権限を有する情報端末であるか否かの端末認証（S2）に加えて、交信可能エリア内に位置する端末であるか否かという端末位置認証又はエリア認証（S3）が行われる。

【0054】

コンテンツデータが購入されていない場合でも、再生が許可された情報端末20である場合（S2：YES）又は交信エリア内に位置する情報端末20である場合（S3：YES）は、試用モードに以降し、ライセンスが発行される（S5）。そして、ライセンスが発行されて再生が開始されたことを使用権管理データベース14に反映させ（S6）、コンテンツデータを復号化して再生する（S7）。

【0055】

そして、コンテンツデータ30に設定されている再生条件が許す範囲内で、コンテンツデータを再生する（S8）。例えば、5分間のみ試聴可、3ページだけ閲覧可等のように、予め許可された範囲内での再生が行われるまで再生部32は待機し、許可された範囲内での再生が行われた場合は（S8：YES）、ライセンスを削除し（S9）、再生が完了したことを使用権管理データベース14に反映させる（S10）。

【0056】

一方、購入済みのユーザである場合は（S1：YES）、コンテンツデータ購入時に使用した情報端末であるか否かを判定する（S11）。コンテンツデータの購入時とコンテンツデータの再生時の情報端末20が一致している場合は（S11：NO）、ライセンスを発行する（S5）。

【0057】

また、過去にそのコンテンツデータを購入したユーザであっても、他の情報端末20で新たに再生しようとする場合は（S11：YES）、コンテンツ購入処理に移行し、再度のコンテンツ購入を促す（S4）。但し、これは、コンテンツ利用権を端末毎に販売する場合であって、端末の種類を問わずに一度購入したコンテンツデータの自由な利用を認めるような場合には、S11を省略し、購入済みユーザであると判断された場合は、ライセンスを発行させてもよい。

【0058】

なお、コンテンツデータが未購入であり（S1：N

O）、予め再生が許可されている端末でもなく（S2：NO）、さらに、情報端末20が所定の交信エリア内に位置していない場合は（S3：NO）、ユーザにコンテンツデータの購入を促す（S4）。

【0059】

コンテンツデータの購入処理では、例えば、購入しようとするコンテンツをユーザが明示的に指定し、クレジットカード決済、電子マネー決済、銀行振込等の決済方法を選択し、所定の個人情報を入力することにより完了する。

【0060】

次に、図5は、コンテンツデータ30の認証部33により実行される認証処理のフローチャートである。

【0061】

コンテンツデータ30がユーザの情報端末20にダウンロードされると、認証部33は自動的に起動する（S21）。認証部22は、ライセンスをサーバ10から情報端末20にダウンロードさせた後（S22）、サーバ10の認証処理部13との間で所定の認証を行う（S23）。認証処理が成功した場合は、所定の時間待ちを行い（S25）、所定の時間が経過した時は再度ライセンスをダウンロードし（S22）、サーバ10との間で認証を行う（S23、S24）。

【0062】

ユーザの情報端末20がサーバ10と交信可能な圏内に位置する間は、情報端末20とサーバ10との間で正常に認証処理が行われるが、ユーザの情報端末20が交信可能圏外に移動した場合は、サーバ10と情報端末20との間で通信を行うことができないため、認証処理が失敗する（S24：NO）。

【0063】

情報端末20とサーバ10との間で通信が行えず、認証が失敗した場合は、削除部34に予め設定されている削除フラグの内容を検査する（S26）。削除フラグは、情報端末20でのコンテンツデータの再生を禁止するモードを指定する情報であり、本実施の形態では、認証失敗後に直ちに削除する第1の削除モードと、認証失敗後に現在の再生終了を待ってから削除する第2のモードとを用意してある。

【0064】

認証部33は、削除フラグによって指定された削除モードが第1のモードか第2のモードかを判定し（S27）、再生終了を待ってから削除する第2のモードを指定されている場合は（S27：YES）、コンテンツデータ30が再生中か否かを判定する（S28）。再生中である場合は、現在の再生が完了するまで時間待ちを行う（S29）。ここで、コンテンツデータ30全体の再生が完了するのを待たずに、コンテンツデータ30のうち一部分の再生完了を待ってから削除するようにしてもよい。例えば、複数の独立した短編から構成されている

書籍コンテンツや複数の独立した楽曲データから構成されている音楽コンテンツの場合等には、現在閲覧中又は試聴中の部分の再生を完了した後で削除し、他の未読部分又は未試聴部分の閲覧を禁止するようにしてもよい。

【0065】

コンテンツデータ30の再生が完了した場合（S28：NO）又は認証失敗後に直ちに削除する第1の削除モードが指定されていた場合（S27：NO）は、認証部33は、ライセンスを破棄し（S30）、削除部34を起動させる（S31）。

【0066】

図6は、削除部34により実行される削除処理を示すフローチャートである。認証部33によって削除部34が起動されると、削除部34は、コンテンツデータ30の全体を削除するためのプログラム（例えばスクリプト）を生成し、カレントディレクトリに配置する（S41）。

【0067】

次に、削除部34は、削除プログラムを起動させ（S42）、削除部自身の実行を終了する（S43）。

【0068】

このようにして削除部34により起動された削除プログラムは、削除部34の起動状態を確認し（S51）、削除部34の起動が終了するまで待機する（S52、S53）。削除部34の実行が終了すると（S52：NO）、削除プログラムは、コンテンツデータ30の全体を削除する（S54）。

【0069】

なお、認証が失敗した場合に、ライセンスが既に破棄されているため、コンテンツデータ30を削除しなくても、その再生を行うことはできない。従って、交信エリア外に出た情報端末20でのコンテンツの利用を阻止するという目的は既に達成されており、図6に示す削除処理は必ずしも必要ではない。

【0070】

しかしながら、削除処理を行うことにより、不正な再利用をより強固に防止することができ、コンテンツ管理システムの信頼性が高まる。一方、ライセンスのみを削除し、コンテンツデータ30を削除しない場合は、ライセンスのみを情報端末20に再びダウンロードするだけで、コンテンツデータ30を再度利用することができる。

【0071】

このように構成される本実施の形態によれば、汎用の情報端末20を用いてコンテンツデータの配信及び管理を行うことができるため、専用端末を用いる場合よりも安価かつ容易にシステムを構築することができる。特に、ストリーミング方式ではなく、情報端末20内にコンテンツデータ30の全体を予め格納させてから再生させるダウンロード方式を採用するため、サーバ10を安価に

構築することができる。また、ネットワークトラフィックが変動した場合でもコンテンツ再生の質に影響がなく、安定した品質を提供できる。

【0072】

また、ユーザが施設1の外部に移動した場合は、ユーザの情報端末20に格納されたコンテンツデータ30の再生を禁止するため、不正なコピーや改ざん等を未然に防止することができる。デジタル化されたコンテンツデータは、従来の物理的媒体に依存する著作物とは異なり、複製や改ざん等が容易であるという特徴を有する。しかし、暗号化等の保護対策が適用されたコンテンツデータを不正にコピー等するには、特殊なソフトウェアや情報端末20よりも処理能力の高いコンピュータ等を用いる必要がある。ユーザが携帯する情報端末20は、通常の場合、データ処理能力の低いコンピュータ装置であるから、施設1外へのコンテンツデータの持ち出しを未然に禁止するだけでも安全性が高まる。

【0073】

さらに、ユーザの情報端末20が施設1の内外いずれに位置するかによってコンテンツデータ30の利用を制御することができるため、施設1外でのコンテンツ利用を制限したい場合等に有効である。例えば、学校等での講義にのみ使用するという条件で著作権者の了解を得てコンテンツデータを配信する場合に、講義外でのコンテンツデータの無断利用を未然に阻止することができる。従って、デジタル化されたコンテンツデータの利用の可能性を広げることができる。

【0074】

本発明を適用可能なビジネスモデルの例を幾つか列挙すると、例えば、音楽ディスク店や書店等では、来店したユーザの情報端末20にユーザが希望する音楽や書籍のコンテンツデータ30を配信して試聴や立ち読み等を許可させることができ、ユーザが店外に出た場合はコンテンツデータ30の利用を禁止することができる。また、例えば、図書館や学校などでは、館内や学校内にいるユーザにのみコンテンツデータ30の利用を許可することができる。

【0075】

2. 第2の実施の形態

【0076】

次に、図7及び図8に基づいて本発明の第2の実施の形態を説明する。本実施の形態の特徴は、情報端末20が位置特定機能（GPS：Global Positioning System）を内蔵又は外付けで利用可能な場合に、GPSにより得られた位置情報も利用して施設1の内外いずれに位置するかを判断する点にある。

【0077】

図7に示すように、コンテンツデータ30内には、情報端末20のGPS機能を利用して位置情報を収集するGPS部35が設けられている。

【0078】

図8に示すように、認証部33は、サーバ10との認証が成功した場合に（S24：YES）、GPS部35からの位置情報に基づいて、情報端末20の現在位置が許可されたコンテンツ利用エリア内に位置するか否かを判定する（S60）。サーバ10との認証が成功した場合でも、情報端末20が所定のエリア外に位置する場合は（S60：NO）、上述の通り、コンテンツデータ30の利用が禁止される（S26～S31）。

【0079】

本実施の形態では、情報端末20と施設1との位置関係を、サーバ10と情報端末20との間の通信による認証とGPS機能による位置情報とで2重に判定するため、施設外部でのコンテンツ利用をより一層効果的に阻止できる。

【0080】

なお、本発明は、上述した実施の形態に限定されない。当業者であれば、前記各実施の形態に構成要素を追加したり、削除したり、変更等したりして種々の変形を行うことができる。

【0081】

例えば、コンテンツサーバから無線LANを介してコンテンツデータを情報端末に供給する場合に限らず、CD-ROM、DVD-ROM、PCカード、メモリ等の記録媒体を介して情報端末にコンテンツデータを供給するようにしてもよい。記録媒体を介して情報端末に供給されたコンテンツデータでも、上記実施の形態と同様に、コンテンツ管理装置と定期的又は不定期に交信し、情報端末の所在を確認してコンテンツデータの利用を制御することができる。

【0082】

【発明の効果】

以上説明した通り、本発明に係るコンテンツ管理システムによれば、ユーザの情報端末が所定の圏内に位置する場合にコンテンツデータの利用を許可し、端末が圏外に出た場合はコンテンツデータの利用を禁止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係るコンテンツ管理システムの全体構成を示すブロック図である。

【図2】コンテンツデータとライセンスとの関係を示す模式図である。

【図3】各データベースの記憶構造を示す説明図である。

【図4】再生処理を示すフローチャートである。

【図5】認証処理を示すフローチャートである。

【図6】削除処理を示すフローチャートである。

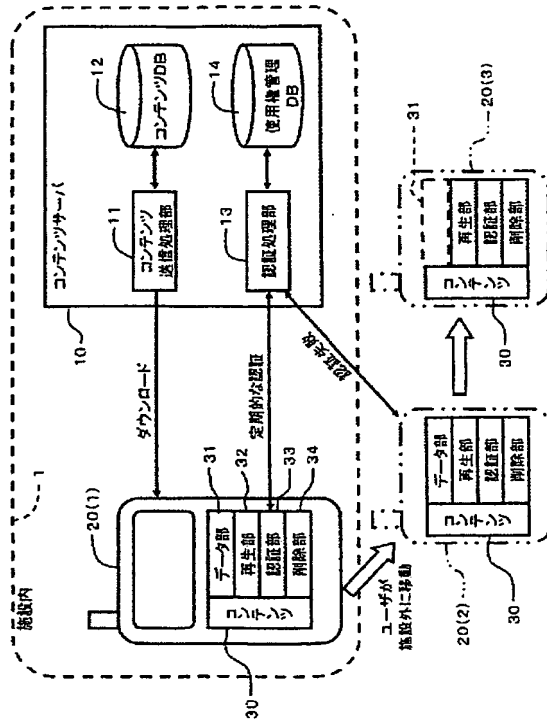
【図7】本発明の第2の実施の形態に係るコンテンツ管理システムの全体構成を示すブロック図である。

【図8】認証処理を示すフローチャートである。

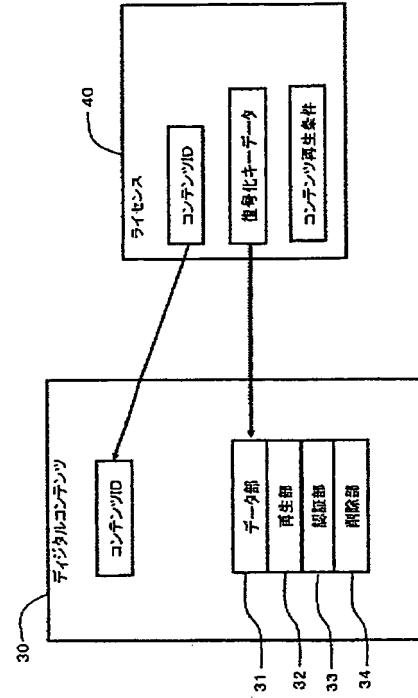
【符号の説明】

- | | | |
|----|----|-------------|
| 20 | 1 | 施設 |
| | 10 | コンテンツサーバ |
| | 11 | コンテンツ送信処理部 |
| | 12 | コンテンツデータベース |
| | 13 | 認証処理部 |
| | 14 | 使用権管理データベース |
| | 20 | 情報端末 |
| | 30 | コンテンツデータ |
| | 31 | データ部 |
| | 32 | 再生部 |
| 30 | 33 | 認証部 |
| | 34 | 削除部 |
| | 35 | GPS部 |

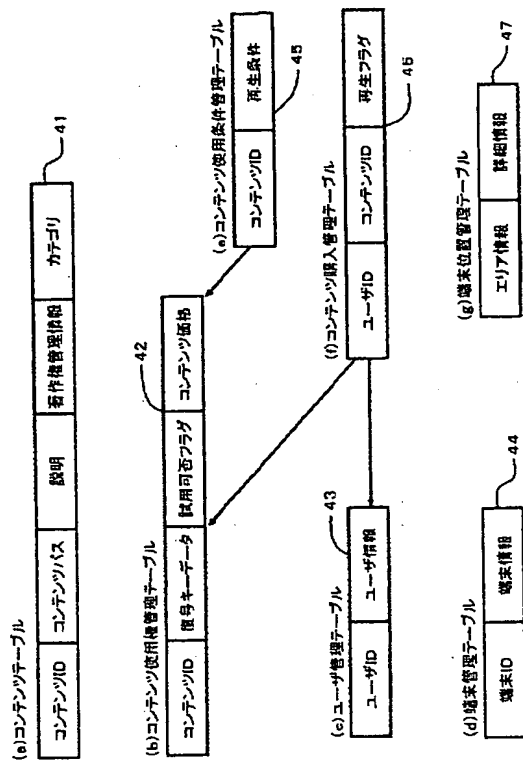
【図1】



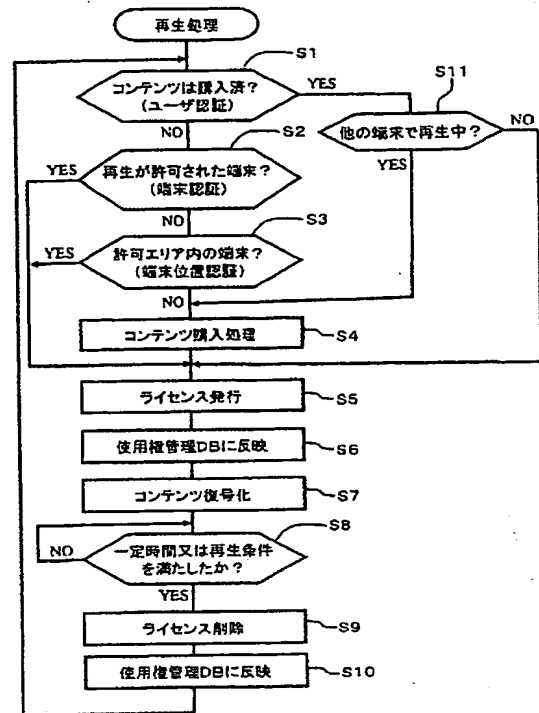
【図2】



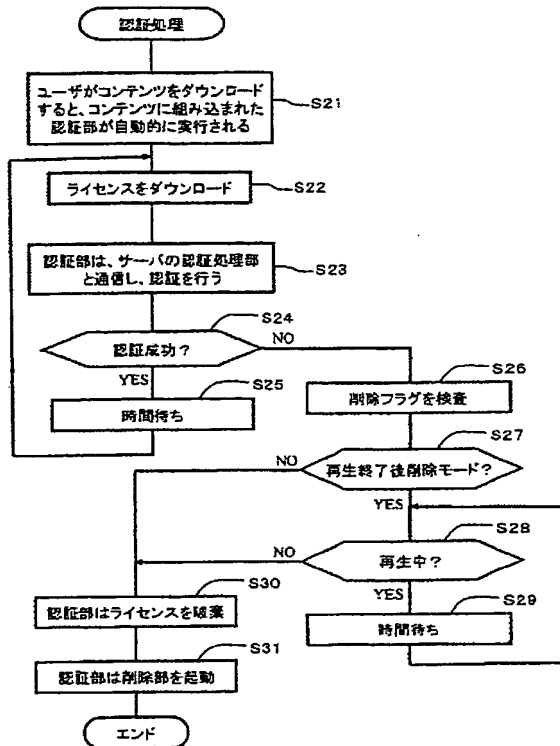
【図3】



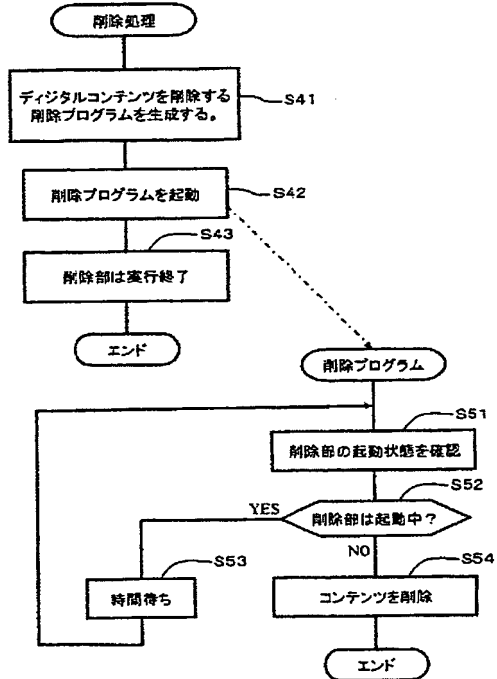
【図4】



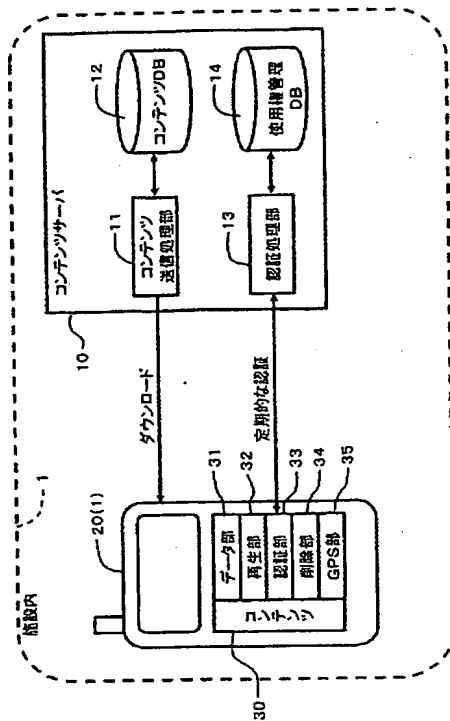
【図5】



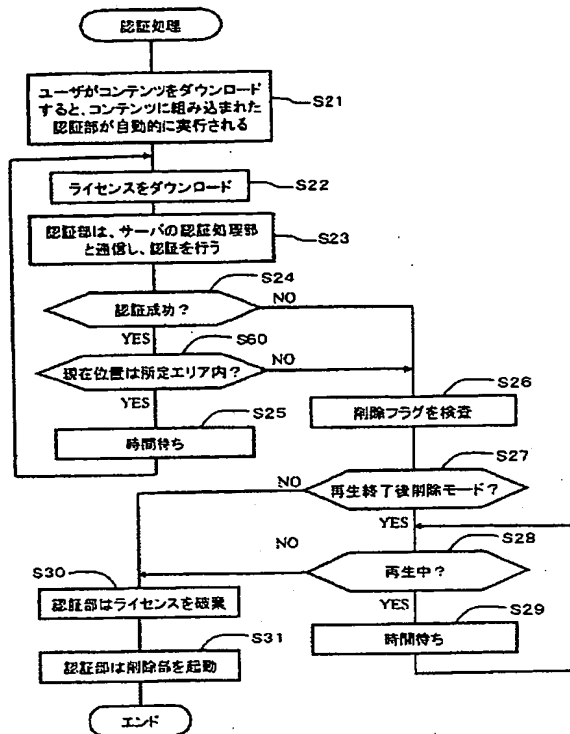
【図6】



【図7】



【図8】



フロントページの続き

(51) Int. Cl.⁷

F I

テーマコード (参考)

H 0 4 Q 7/04

Z

H 0 4 B 7/26

M

THIS PAGE BLANK (USPTO)